EVALUATING INITIALLY UNTRUSTED EVIDENCE
IN AN EVIDENCE-BASED SECURITY POLICY MANAGER

Abstract of the Invention

An evidence-based policy manager generates a permission grant set for a code assembly

5   received from a resource location. The policy manager executes in a computer system (e.g., a

Web client or server) in combination with the verification module and class loader of the run-

time environment. The permission grant set generated for a code assembly is applied in the run-

time call stack to help the system determine whether a given system operation by the code

assembly is authorized. Both code assemblies and evidence may be received from a local origin

10   or from a remote resource location via a network (e.g., the Internet). Evidence having different

levels of trust may be evaluated in combination so that a permission grant set is associated only

with trusted code assemblies. The policy manager may comprise execution modules for parsing

a security policy specification, generating one or more code hierarchies, evaluating membership

of the received code assembly in one or more code groups, and generating a permission grant set

15   based upon this membership evaluation.